

POC DMZ - Rapport de mise en service

Table des matières

POC DMZ - Rapport de mise en service

Table des matières

User Story 7

Test d'acceptation

User Story 8

Test d'acceptation

User Story 9

Test d'acceptation

User Story 7

Test d'acceptation

- Schéma avec différents flux

Networks

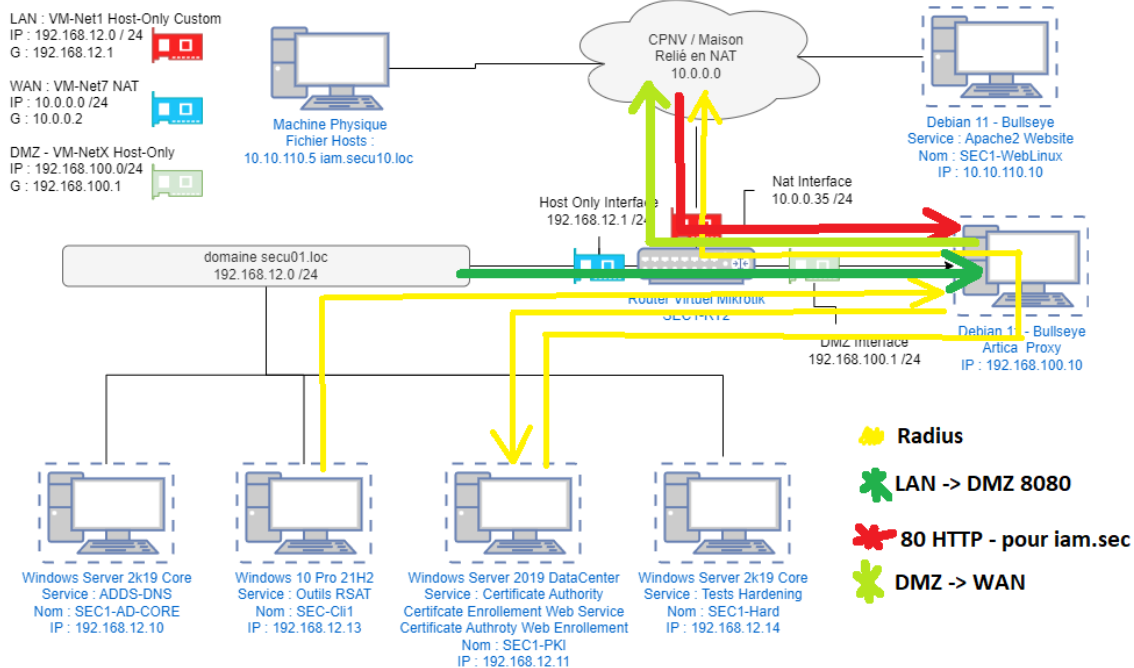


Tableau des actions

- Identique a Rapport 1 - DMZ
































Tableau règles firewall

Source	Destination	Protocol	Act
All	All	ICMP	Accept
192.168.12.0/24	192.168.100.10:8080	TCP/UDP Squid	Accept
192.168.12.0/24	192.168.12.1	Any	Accept
192.168.12.0/24	192.168.100.10/24:22	TCP/UDP SSH	Accept
192.168.12.0/24	Any	Any	Drop
All	192.168.100.10:80	TCP HTTP	Accept
192.168.100.0/24	Any :443	TCP/UDP HTTPS	Accept
192.168.100.0/24	Any :80	TCP/UDP HTTP	Accept
192.168.100.0/24	Any :53	TCP/UDP DNS	Accept
192.168.100.0/24	192.168.12.11:1812	TCP/UDP RADIUS	Accept
192.168.100.0/24	192.168.12.11:1813	TCP/UDP RADIUS ACCOUNTING	Accept

Images avec règles firewall



















Firewall: Rules: LAN Select category

Select category

<input type="checkbox"/>		Protocol	Source	Port	Destination	Port	Gateway	Schedule		Description 
										Automatically generated rules
<input type="checkbox"/>	  	IPv4 *	LAN net	*	*	*	*	*		Default allow LAN to any rule
<input type="checkbox"/>	  	IPv4 TCP/UDP	LAN net	*	DMZ net	8080	*	*		
<input type="checkbox"/>	  	IPv4 *	LAN net	*	This Firewall	*	*	*		
<input type="checkbox"/>	  	IPv4 ICMP	*	*	*	*	*	*		
<input type="checkbox"/>	  	IPv4 TCP/UDP	LAN net	*	192.168.100.10/24	22 (SSH)	*	*		
<input type="checkbox"/>	  	IPv4 *	LAN net	*	*	*	*	*		
	pass		block			reject			log	 in
	pass (disabled)		block (disabled)			reject (disabled)			log (disabled)	 out

Firewall: Rules: WAN Select

Select

<input type="checkbox"/>	Protocol	Source	Port	Destination	Port	Gateway	Schedule	
<input type="checkbox"/>								
<input type="checkbox"/>	   	IPv4 *	*	*	*	*	*	
<input type="checkbox"/>	   	IPv4 TCP	*	*	192.168.100.10	80 (HTTP)	*	*
	pass		block		reject		log	
	pass (disabled)		block (disabled)		reject (disabled)		log (disabled)	
	Active/Inactive Schedule (click to view/edit)							

Firewall: Rules: DMZ

<input type="checkbox"/>	Protocol	Source	Port	Destination	Port	Gateway	Schedule	
<input type="checkbox"/>	IPv4 *	*	*	*	*	*	*	
<input type="checkbox"/>	IPv4 TCP/UDP	DMZ net	*	*	443 (HTTPS)	*	*	
<input type="checkbox"/>	IPv4 TCP/UDP	DMZ net	*	*	80 (HTTP)	*	*	
<input type="checkbox"/>	IPv4 TCP/UDP	DMZ net	*	*	53 (DNS)	*	*	
<input type="checkbox"/>	IPv4 TCP/UDP	DMZ net	*	192.168.12.11	1812 (RADIUS)	*	*	
<input type="checkbox"/>	IPv4 TCP/UDP	DMZ net	*	192.168.12.11	1813 (RADIUS accounting)	*	*	
<input type="checkbox"/>	pass	<input checked="" type="checkbox"/> block		<input checked="" type="checkbox"/> reject		<input checked="" type="checkbox"/> log		<input type="button" value="→"/>
<input type="checkbox"/>	pass (disabled)	<input checked="" type="checkbox"/> block (disabled)		<input checked="" type="checkbox"/> reject (disabled)		<input checked="" type="checkbox"/> log (disabled)		<input type="button" value="←"/>
<input type="button" value="📅"/> <input type="button" value="📅"/> Active/Inactive Schedule (click to view/edit)								

Test d'accès internet en direct (sans proxy)

- Image doit montrer que ce n'est pas possible, par exemple un ping vers un site externe

Test d'accès à Internet par le proxy

- Image doit montrer que c'est possible à l'aide du proxy
- wget www.google.ch avec proxy : Demande de authentification
- wget sans proxy : non résolu

Proxy

Configuration manuelle du proxy

Utilisez un serveur proxy pour les connexions Ethernet ou Wi-Fi. Ces paramètres ne s'appliquent pas aux connexions VPN.

Utiliser un serveur proxy

☐ Désactivé

Adresse: 192.168.100.10 Port: 8080

Utilisez le serveur proxy sauf pour les adresses qui commencent par les entrées suivantes. Utilisez des points-virgules (;) pour séparer les entrées.

192.168.12.*

☐ Ne pas utiliser le serveur proxy pour les adresses (intranet) locales

Administrateur : Windows PowerShell

```
Windows PowerShell
Copyright (C) Microsoft Corporation. Tous droits réservés.

Testez le nouveau système multiplateforme PowerShell https://aka.ms/powershell

PS C:\Users\Administrateur> wget www.google.ch
wget : ERROR
Cache Access Denied.
The following error was encountered while trying to retrieve the URL: http://www.google.ch/
Cache Access Denied.
Sorry, you are not currently allowed to request http://www.google.ch/ from this cache until you have authenticated yourself.
Please contact the cache administrator if you have difficulties authenticating yourself.
Generated Wed, 06 Dec 2023 08:26:29 GMT by srsrpxy (squid/5.7)
Au caractère Ligne:1 : 1
+ wget www.google.ch
+ ~~~~~
+ CategoryInfo          : InvalidOperation : (System.Net.HttpWebRequest:HttpWebRequest) [Invoke-WebRequest], WebEx
ception
+ FullyQualifiedErrorId : WebCmdletWebResponseException,Microsoft.PowerShell.Commands.InvokeWebRequestCommand

PS C:\Users\Administrateur> wget www.google.ch
wget : Le nom distant n'a pas pu être résolu: 'www.google.ch'
Au caractère Ligne:1 : 1
+ wget www.google.ch
+ ~~~~~
+ CategoryInfo          : InvalidOperation : (System.Net.HttpWebRequest:HttpWebRequest) [Invoke-WebRequest], WebEx
ception
+ FullyQualifiedErrorId : WebCmdletWebResponseException,Microsoft.PowerShell.Commands.InvokeWebRequestCommand

PS C:\Users\Administrateur>
```

User Story 8

Test d'acceptation

Utilisateurs et ordinateurs Active Directory

Fichier Action Affichage ?

Utilisateurs et ordinateurs Active Directory

- Requêtes enregistrées
- Secu01.loc
 - Builtin
 - Computers
 - Domain Controllers
 - ForeignSecurityPrincipals
 - Managed Service Accounts
 - SEC1
 - Server Hardening
 - Users

Nom	Type
Administrateur	Utilisateur
Administrateurs clés	Groupe de...
Administrateurs clés Enterprise	Groupe de...
Administrateur	
Administrateur	
Admins de...	
Contrôleu...	
Contrôleu...	
Contrôleu...	
Contrôleu...	
Contrôleu...	
DGS	
DnsAdmini...	
DnsUpdat...	
Éditeurs d...	

Propriétés de : DGS

Environnement	Sessions	Contrôle à distance	Profil des services Bureau
Général	Adresse	Compte	Profil
			Téléphones
			Organis...

Membre de :

Nom	Dossier Services de domaine Active Directory
NetAdmin	Secu01.loc/Users
Utilisateurs du do...	Secu01.loc/Users

Serveur NPS (Network Policy Server)

Fichier Action Affichage ?

NPS (Local)

- Clients et serveurs RADIUS
 - Clients RADIUS
 - Groupes de serveurs RA...
- Stratégies
 - Stratégies de demande
 - Stratégies réseau
- Gestion
 - Secrets partagés
 - Clients RADIUS
 - Serveurs RADIUS distan...
 - Filtres IP

Stratégies réseau

Les stratégies réseau vous permettent d'autoriser les connexions au réseau de manière...

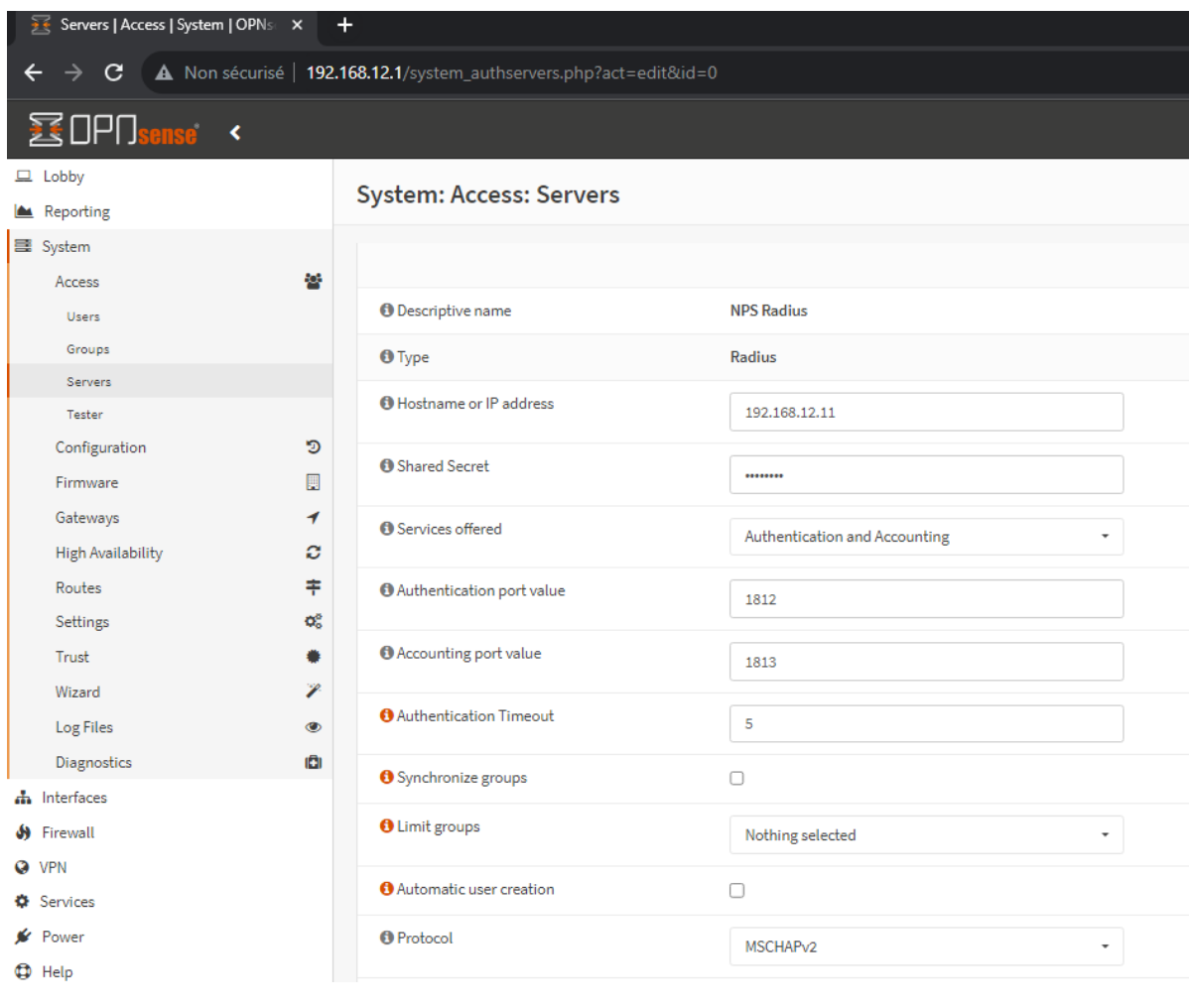
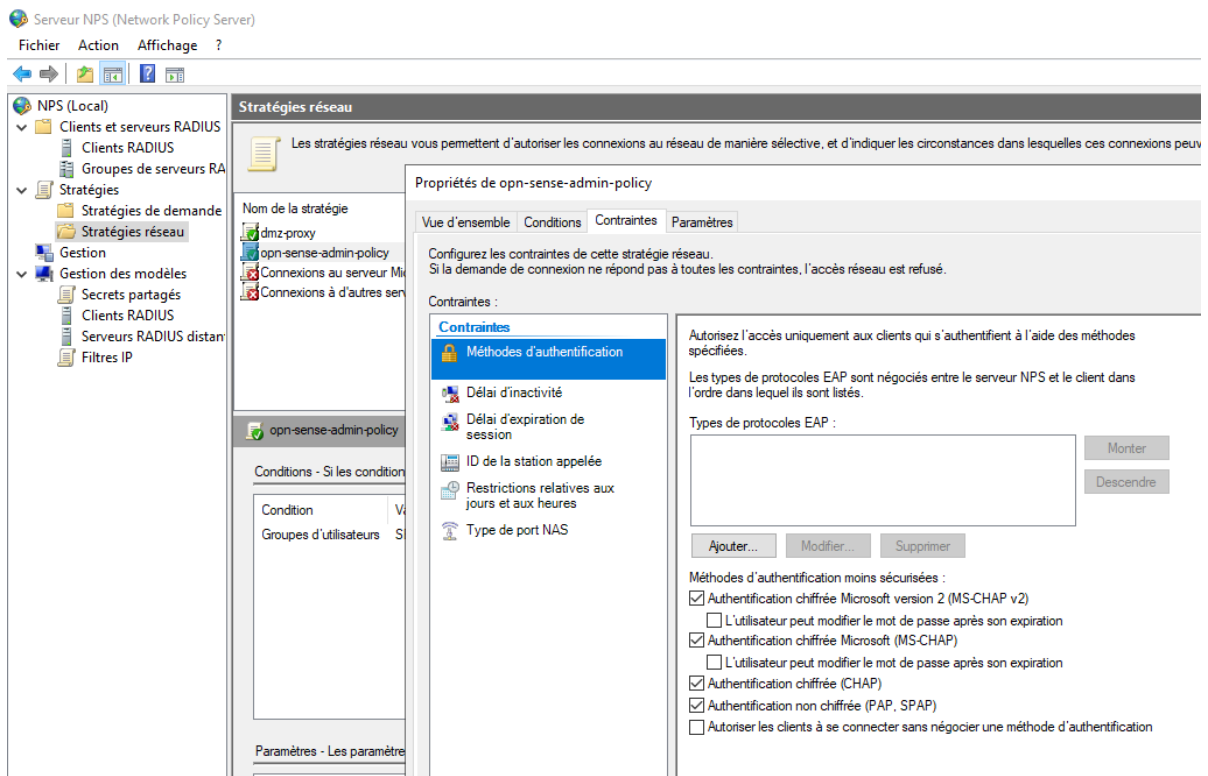
Propriétés de opn-sense-admin-policy

Vue d'ensemble Conditions Contraintes Paramètres

Configurez les conditions de cette stratégie réseau.

Si la demande de connexion répond aux conditions, le serveur demande de connexion ne répond pas aux conditions, le serveur stratégies supplémentaires seraient configurées.

Condition	Valeur
Groupes d'utilisateurs	SECU01\NetAdmin



Tester | Access | System | OPNsense

Non sécurisé | 192.168.12.1/diag_authentication.php

OPNsense

Lobby

Reporting

System

- Access
- Users
- Groups
- Servers
- Tester

Configuration

- Firmware
- Gateways
- High Availability
- Routes
- Settings
- Trust
- Wizard
- Log Files
- Diagnostics

System: Access: Tester

User: DGS@secu01.loc authenticated successfully.
This user is a member of these groups:

Attributes received from server:
class => admins
A+wx(x\

Authentication Server

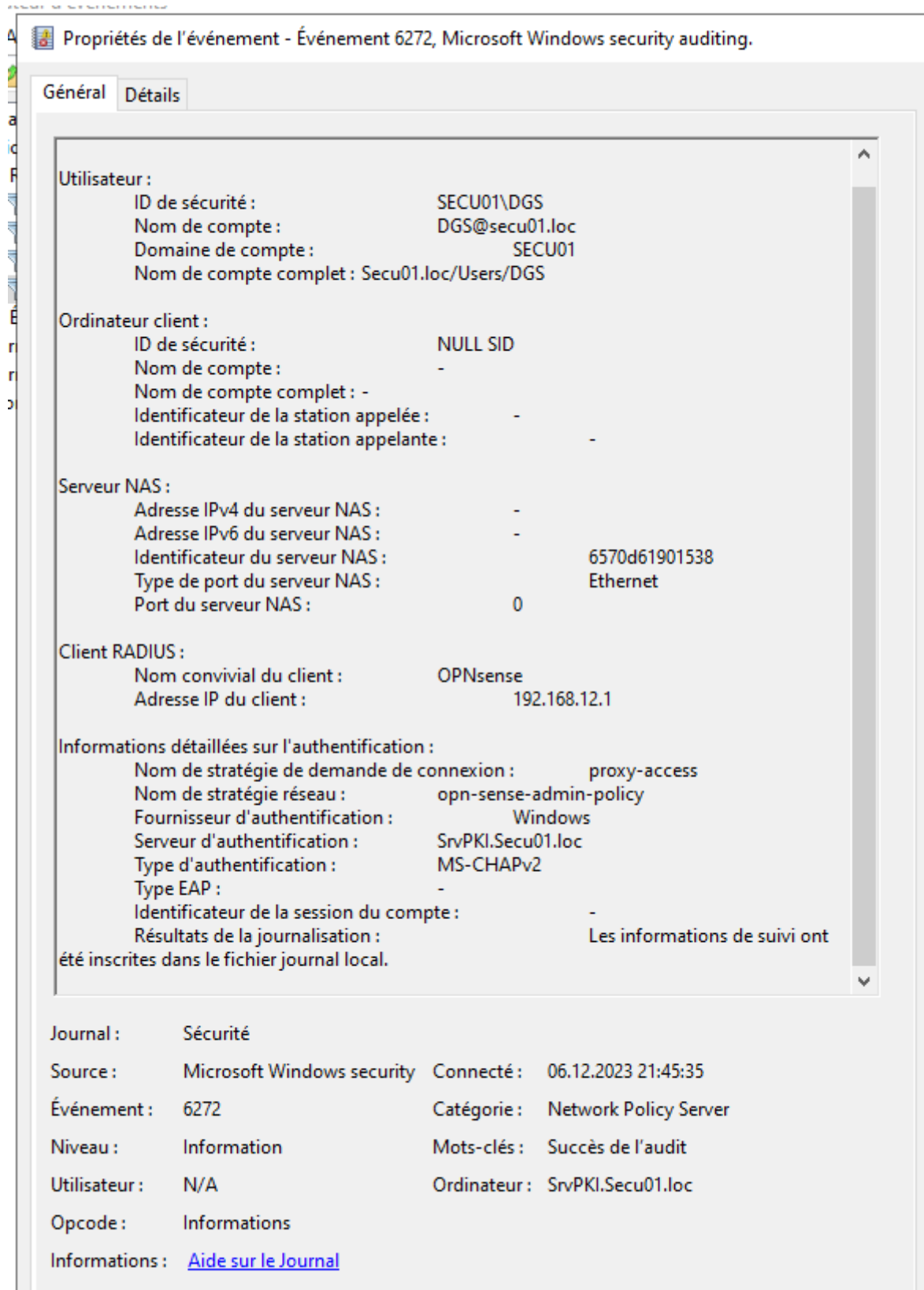
NPS Radius

Username

DGS@secu01.loc

Password

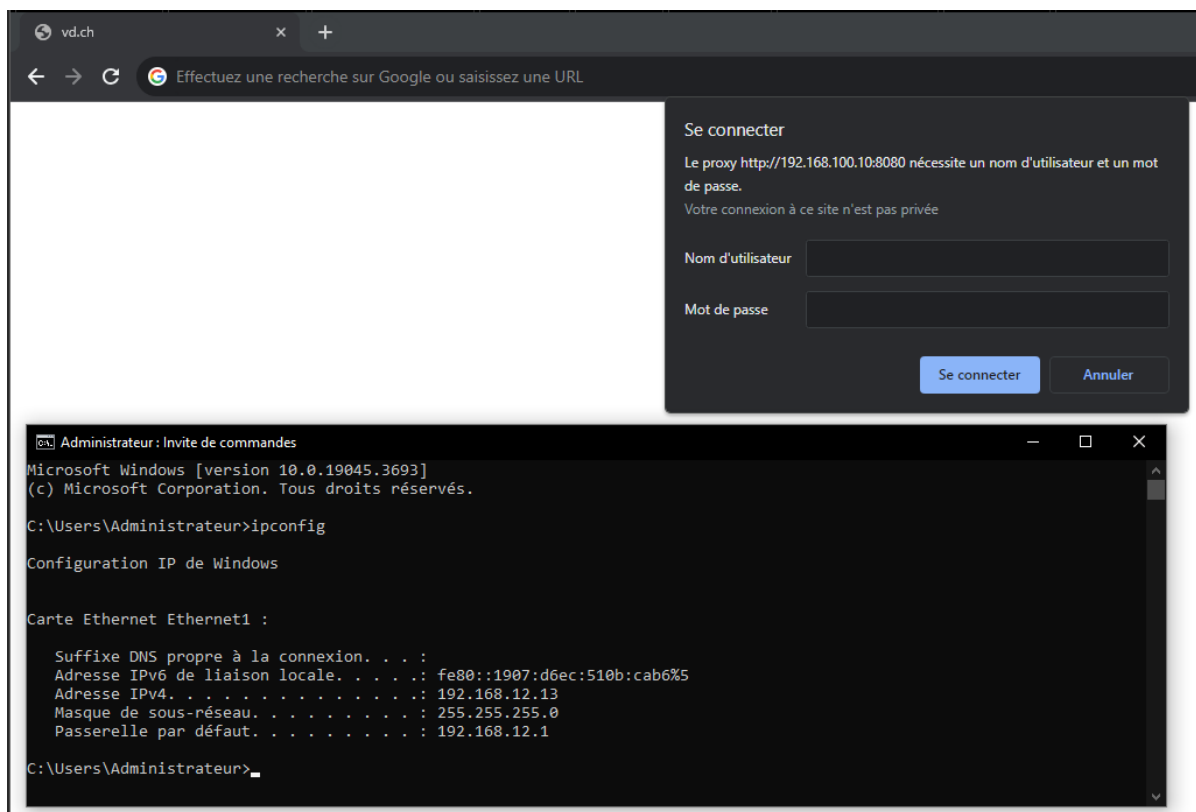
Test



User Story 9

Test d'acceptation

Accès authentifié au proxy



Config du fichier /etc/squid/squid.conf : Configuré dans conf.d pour savoir mieux ce que on rajoute

```
cpnv@srvprxy:/etc/squid/conf.d$ cat sec2.conf
#Proxy Auth
auth_param basic program /usr/lib/squid/basic_radius_auth -f
/etc/squid/radius.conf
auth_param basic children 5
auth_param basic realm Web-Proxy
auth_param basic credentialsttl 5 minute
auth_param basic casesensitive off

# HTTP Port
http_port 192.168.100.10:8080
cache_dir ufs /var/spool/squid 100 16 256

# ACL List
acl lanet src 192.168.12.0/24
acl dmznet src 192.168.100.0/24
acl whitelist dstdomain "/etc/squid/conf.d/sites.whitelist.txt"
acl radius-auth proxy_auth REQUIRED

# Access list
# http_access allow lanet
# http_access allow dmznet
# http_access allow whitelist
http_access allow radius-auth whitelist

# Blacklist
http_access deny all
```

Observateur d'événements sur la PKI

Propriétés de l'événement - Événement 6272, Microsoft Windows security auditing.

Général Détails

Le serveur NPS a accordé l'accès à un utilisateur.

Utilisateur :

- ID de sécurité : SECU01\Jan
- Nom de compte : jan
- Domaine de compte : SECU01
- Nom de compte complet : Secu01.loc/Users/Jan

Ordinateur client :

- ID de sécurité : NULL SID
- Nom de compte : -
- Nom de compte complet : -
- Identificateur de la station appelée : -
- Identificateur de la station appelante : -

Serveur NAS :

- Adresse IPv4 du serveur NAS : 192.168.100.10
- Adresse IPv6 du serveur NAS : -
- Identificateur du serveur NAS : -
- Type de port du serveur NAS : Asynchrone
- Port du serveur NAS : 111

Client RADIUS :

- Nom convivial du client : srpxpy
- Adresse IP du client : 192.168.100.10

Informations détaillées sur l'authentification :

- Nom de stratégie de demande de connexion : proxy-access
- Nom de stratégie réseau : dmz-proxy
- Fournisseur d'authentification : Windows
- Serveur d'authentification : SrvPKI.Secu01.loc
- Type d'authentification : PAP
- Type EAP : -
- Identificateur de la session du compte : -
- Résultats de la journalisation : Les informations de suivi ont été inscrites dans le fichier journal local.

Journal : Sécurité

Source : Microsoft Windows security Connecté : 06.12.2023 20:33:21

Événement : 6272 Catégorie : Network Policy Server

Niveau : Information Mots-clés : Succès de l'audit

Utilisateur : N/A Ordinateur : SrvPKI.Secu01.loc

Opcode : Informations

Informations : [Aide sur le Journal](#)

Logs Squid

```

cpnv@srpxpy:~$ sudo tail -f /var/log/squid/access.log
1701891208.447 0 192.168.12.13 TCP_DENIED/403 4090 CONNECT www.google-analytics.com:443 jan HIER_NONE/- text/html
1701891208.448 0 192.168.12.13 TCP_DENIED/403 4090 CONNECT www.googletagmanager.com:443 jan HIER_NONE/- text/html
1701891208.778 0 192.168.12.13 TCP_DENIED/403 4111 CONNECT content-autofill.googleapis.com:443 jan HIER_NONE/- text/html
1701891209.704 0 192.168.12.13 TCP_DENIED/403 4111 CONNECT content-autofill.googleapis.com:443 jan HIER_NONE/- text/html
1701891211.185 0 192.168.12.13 TCP_DENIED/403 4111 CONNECT content-autofill.googleapis.com:443 jan HIER_NONE/- text/html
1701891213.924 0 192.168.12.13 TCP_DENIED/403 4111 CONNECT content-autofill.googleapis.com:443 jan HIER_NONE/- text/html
1701891218.140 0 192.168.12.13 TCP_DENIED/403 4363 GET http://swisssign.net/cgi-bin/authority/download/80F38FD9FC82688153C18
1701891218.142 0 192.168.12.13 TCP_DENIED/403 4363 GET http://swisssign.net/cgi-bin/authority/download/DA34D48E1023F46A2D6C8
1701891220.890 0 192.168.12.13 TCP_DENIED/403 4111 CONNECT content-autofill.googleapis.com:443 jan HIER_NONE/- text/html
1701891312.902 0 192.168.12.13 TCP_DENIED/407 4128 CONNECT config.edge.skype.com:443 - HIER_NONE/- text/html
1701891332.550 123771 192.168.12.13 TCP_TUNNEL/200 7927 CONNECT prestations.vd.ch:443 jan HIER_DIRECT/145.232.192.146 -
1701891332.550 124102 192.168.12.13 TCP_TUNNEL/200 74628 CONNECT statsweb.vd.ch:443 jan HIER_DIRECT/145.232.192.131 -
1701891332.550 124197 192.168.12.13 TCP_TUNNEL/200 575452 CONNECT www.vd.ch:443 jan HIER_DIRECT/145.232.192.197 -
1701891332.550 124105 192.168.12.13 TCP_TUNNEL/200 178721 CONNECT www.vd.ch:443 jan HIER_DIRECT/145.232.192.197 -
1701891332.550 124105 192.168.12.13 TCP_TUNNEL/200 254526 CONNECT www.vd.ch:443 jan HIER_DIRECT/145.232.192.197 -
1701891332.550 124105 192.168.12.13 TCP_TUNNEL/200 178264 CONNECT www.vd.ch:443 jan HIER_DIRECT/145.232.192.197 -
1701891332.550 132147 192.168.12.13 TCP_TUNNEL/200 1160857 CONNECT www.vd.ch:443 jan HIER_DIRECT/145.232.192.197 -
1701891332.550 124197 192.168.12.13 TCP_TUNNEL/200 1934281 CONNECT www.vd.ch:443 jan HIER_DIRECT/145.232.192.197 -

```